

**ENHANCING THE SECURITY OF HAZARDOUS MATERIAL PETROLEUM
SHIPMENTS AGAINST ACTS OF TERRORISM OR SABOTAGE**
(VIA THE UNITED STATES DEPARTMENT OF TRANSPORTATION'S RESEARCH AND SPECIAL PROGRAMS ADMINISTRATION)

RISK MANAGEMENT ASSESSMENT PLANNING GUIDE

Introduction

Given the heightened specter of terrorism, the security of petroleum shipments and other hazardous materials has become a priority for petroleum marketers, carriers, shippers, consignees, emergency responders and government officials. The existing hazardous material transportation process, including personnel, procedures, cargo tank motor vehicles and bulk plant facilities must be reexamined from a security prospective. Addressing security concerns should be part of an overall strategy to manage the risk of hazardous materials, such as petroleum products, during transportation.

The following risk assessment tool can be used to aid petroleum marketers in enhancing security and safeguard shipments of petroleum products against terrorist attack or sabotage. This risk assessment document will help to evaluate and manage risks and hone practical, common sense knowledge to reduce risk even further.

I. Principles Applied to Managing Security Risk

The following fundamental principals are critical for successfully managing risk:

- Obtaining commitment to reducing security risks on the part of both managers and workers.
- Promoting a “risk reduction culture with a security focus” in day-to-day operations.
- Partnering with all parties involved in securing the petroleum transport distribution chain.
- Prioritizing security risks so that resources can be allocated effectively.
- Taking action to reduce the security risks that have been identified.
- Striving for continuing improvement.
- Communicating with all parties to ensure each knows its role and is aware of relevant security risk information.

II. Step-by-Step Process for Security Risk Assessment

Step 1: Defining the Scope of Security Requirements –What’s Covered?

Security considerations can cut across the entire petroleum transportation process. However, to effectively focus an effort on security risk, a company should generally characterize its petroleum transportation process, and then make initial decisions as to which transportation activities merit more security scrutiny. The initial decisions may be made based on company perceptions of the greatest security risks or based on previous threats. Key areas of concern for petroleum marketers are cargo tank and bulk plant security, and personnel

security screening that focuses on U.S. residency status, criminal background history and the validity of CDL licenses, hazardous material endorsements and driver medical qualification certificates.

Defining the scope of the activities to be considered in terms of security also includes identifying other partners that are interested in the security of the company's petroleum shipments. For petroleum marketers, these partners include terminal operators, for-hire motor carriers, cargo tank motor vehicle repair shops, and local law enforcement officials.

Step II: Knowledge of Operations – Making a List

Step II involves collecting detailed information about the petroleum transportation operations/decisions that will be examined for security risks. Make a list. Describe the quantities of petroleum shipped, who handles the product, the routes used for delivery and where and when the product is handled. For petroleum marketers the quantity of product shipped is easily determined from existing company records. HAZMAT drivers and HAZMAT employees are the primary parties handling product, delivery routes are generally well known and the products are essentially handled at the terminal, bulk plant loading rack and at delivery locations.

Additionally, describe on the list the existing security activities already in place for the transportation of petroleum products. Keep in mind that the new security rules issued by the U.S. Department of Transportation includes storage incidental to shipment (i.e. bulk plants). The inventory of information should cover security issues with personnel (background checks, licensing and training), security procedures and plans, and the security of bulk plant facilities and equipment. Current safety and risk regulations (e.g. parking restrictions) that have security impacts are also important to the list. In determining the security activities to describe, ask how loads are secured. Questions such as Do drivers regularly follow the company's security and safety guidelines? What are the chief causes of transportation related accidents? Have any threats previously been received at the company offices? Are there any trends that can be identified (e.g. areas or type of equipment with a high frequency of theft)? Much of the list is really based on *common sense and your intimate knowledge of company operations*.

Step III. Assessment – What are the risks?

This assessment step involves analysis of the company's operations and characterization of the nature and magnitude of the security risks. The assessment does not have to be costly or complex, but can begin simply and progress in complexity as needed. It can simply involve reporting the impressions of experienced company staff, brainstorming sessions, or conducting a survey by a diverse team composed of staff from various operations (e.g. drivers, dispatchers, cargo tank and bulk storage equipment vendors). Generally, small business petroleum marketers fully understand the dangers from both a safety and security standpoint involved with transporting petroleum products. Much of it is based on common sense. The risk assessment process can be made as simple as possible but should be memorialized in writing and kept on file for future U.S. DOT inspections. Use the work attached sheet to assist you in this process.

The goal is to identify points in the petroleum distribution chain where security risks exist, but where actions can be taken to reduce the security risk. Risk control points for petroleum marketers typically include;

- **Personnel Backgrounds** – Employment history and verification of citizenship of HAZMAT drivers and HAZMAT employees.
- **Cargo Tank Motor Vehicle and Bulk Plant Access Control** - Locking procedures for unattended cargo tank motor vehicles and loading rack equipment, secure parking areas, lighting, fences where necessary, security systems, integrity of access codes and key storage, limiting access to authorized personnel.

- **En Route Security** – Avoiding highly urbanized areas, bridges, tunnels, public schools and hospitals. Prohibiting drivers from changing delivery routes without prior authority, maintaining contact with drivers, forbidding unscheduled and unauthorized stops (except if instructed by a law enforcement official), prohibitions stopping for hitchhikers, assisting roadside motorists in need, parking in secure areas, and removing ignition key, locking doors and rolling up windows at all stops, including delivery.
- **Communications** – Use of cell phones or two radios to reach all drivers, immediate reporting of suspicious activities, providing updated information on security to HAZMAT drivers and HAZMAT employees as it becomes available and informing them of national security threat levels set by the U.S. Department of Homeland Security (i.e. the color code threat level system), loading and unloading activities at bulk plants, en route transportation of product to the customer, delivery into the customer’s tank, unattended cargo tank vehicles, ease of and ability to control access to cargo tank vehicles, bulk plant facilities and shipping information, emergency response protocols, and HAZMAT driver and HAZMAT employee criminal, residency and work histories.
- **Emergency Response** – Adequacy of training and resources for response to terrorist type incidents, centralizing emergency response and information through a designated company security contact.
- **Readjustment Based on Changed Circumstances** – Possible Heightened security procedures after terrorist attacks or increased threat levels.

Step IV. Strategy – The Written Security Plan

The heart of a strategy to address security risks is to develop a security action plan. The plan prioritizes the security risk control points based on the degree of vulnerability and potential impact. The written security plan also outlines potential and preventative control actions based on the ability to reduce risk and the resources available. The plan should provide for the installation of new equipment (e.g. locks, lights etc.) if appropriate, establish security procedures, assign security response responsibilities to key employees and convey management commitment to enhanced security awareness and risk reduction procedures.

A written security plan developed for small business petroleum marketers is included in this package. It is designed as a template that can be easily changed to fit specific marketing operations and unique security needs.

Petroleum marketers are likely to find that they are already performing many of these security procedures. For example, the requirement for in depth security training for HAZMAT drivers and HAZMAT employees under the new DOT security regulations has been incorporated into existing DOT training programs these employees must already undergo on a periodic basis. Petroleum marketers should simply make certain that the HAZMAT training provider they are currently using has incorporated the in depth security training component as part of the regular curriculum. Get the verification in writing if possible and place it in your security risk assessment files. Also, HAZMAT driver background checks are conducted by state licensing authorities along with the FBI and DOT, so there is no need for petroleum marketers to duplicate this task. Similarly, most drivers already have cell phones or two-way radios to maintain continual contact with dispatchers or company management. Packaging control such as locks for cargo tanks, bulk plant loading racks and valves and security lights are likely to already be in place.

On the other hand, petroleum marketers should focus on upgrading emergency response capabilities relating to security issues. Since such a system is already in place for safety related emergencies, only minor adjustments to fold in the security component will be required.

Step V. Implementation – Getting the Plan Activated

This step is simple. Familiarize HAZMAT drivers and HAZMAT employees with the security plan, ensure that they fully understand it and are committed to implementing it on a daily basis. Make the plan official company policy and require HAZMAT drivers and HAZMAT employees to sign it, attesting to their awareness of the plan's components and commitment to implementing it at all times.

Step VI. Evaluation – Is the Plan Working?

This step determines if the goals established for reducing security risks are being met. To measure progress, monitor the plan in action and establish performance indicators to evaluate its effectiveness. Evaluate the plan on a periodic basis. When weaknesses are identified change the security plan as needed. Keep written records of your efforts to evaluate the effectiveness of the plan and maintain them in a security file.

Additional Resources:

- 1) **U.S. DOT Hazardous Material Safety Web Page** – Provides the latest government alert on terrorism: <http://hazmat.dot.gov>. More information on security plan development and risk assessment can be found at: <http://hazmat.dot.gov/rmsef.htm>. A training module for HAZMAT drivers and HAZMAT employees may be downloaded for free at: http://hazmat.gov/hmt_security.htm.
- 2) **Federal Motor Carrier Safety Administration Security Talking Web Page** – Security talking points including general security information, personnel security, hazardous materials packaging controls, en route security, technical innovations, management prerogatives, communications and readjustment of plans based on changed conditions can all be found at: www.fmcsa.dot.gov/hazmatsecure.htm.
- 3) **National Cargo Security Council Web Page** – Provides theft prevention information, including a list of cargo security links at: www.cargosecurity.com.
- 4) **National Safety Council Web Page** – Presents general safety information including emergency response plan information at: www.nsc.org/issues/emerg/99esc.htm
- 5) **American Trucking Associations (ATA) Web Page** – Provides information on government security warnings, security tips, security of cargo tank motor vehicles and driver security information at: www.truckline.com.
- 6) **Transportation Research Board Security Web Page** – Provides links to documents and other information on general transportation security at: <http://www4.trb.org/trb/homepage.nsf/web/security>.
- 7) **American Chemistry Council Web Page** – Provides guidance on transportation security and guidelines on chemical plant security at: <http://www.americanchemistry.com>
- 8) The **Petroleum Transportation and Storage Association (PTSA)** – Provides regulatory compliance information regarding all aspects of security planning and other federal regulatory requirements for the petroleum marketing industry. Contact Mark S. Morgan at: ptsa@erols.com or call (703) 281-6600.
- 9.) The **Florida Petroleum Marketers and Convenience Store Association (FPMA)** – Provides members with resources and clarifications regarding this subject matter. Contact: Jim Smith, President/CEO at: jim@fpma.org or call (800) 523-9166